DRAFT
Interim Safety Guidance
for
Reusable Launch Vehicles

Table of Contents

PREFACE

The Associate Administrator for Commercial Space Transportation (AST) has developed draft interim safety guidance for use by an applicant for a license to operate a reusable launch vehicle (RLV). This guidance is intended to assist an applicant in responding to public safety concerns of the agency associated with an application to conduct RLV operations.

The safety objectives presented in this interim safety guidance are not regulations. The guidance reflects the agency's general policy of ensuring public safety is not jeopardized as a result of new launch vehicle technology. Until the FAA issues regulations that address the unique safety aspects associated with reentry of reentry vehicles and Reusable Launch Vehicle (RLV) operations, the FAA will consider license applications for RLV launch and reentry on a case-by-case basis, taking into account the operational capability of a proposed vehicle. Development of a license application by an RLV operator is facilitated through early and frequent consultation between the applicant and the agency to assure public safety issues are identified and adequately addressed by the applicant. To the extent appropriate, existing licensing regulations will apply to applications to launch or reenter an RLV. However, for those unique safety aspects associated with RLV or reentry operations, the FAA is providing this interim safety guidance that reflects public safety concerns of the FAA in evaluating a license applicant's ability to conduct safe launch and reentry operations.

Objective 1: Public Expected Casualty

The public should not be exposed to an unreasonable risk of harm as a result of RLV operations. Risks to public safety will be measured in terms of collective risk, similar to launches from Federal ranges. The risk to the public for Reusable Launch Vehicle (RLV) operations shall not produce a total public casualty expectancy (E_C) greater than that allowed by Federal ranges, that is $30x10^{-6}$ during the launch and reentry phase of a mission. This per mission E_C includes both launch and reentry risks as parts of a single mission.

(The launch and reentry phases of an operation together are regarded as one mission that must satisfy this E_C criterion.)

Discussion:

This objective of limiting expected casualty[1] to 30×10^{-6} for RLV operations is consistent with current guidelines and standards for public risk for launch activities of expendable launch vehicles (ELVs) at Federal (DOD) ranges.[2] It is anticipated that there may be situations where separate launch and reentry operators may be seeking licenses for operations that result from the same mission event. This objective considers that ascent and reentry are effectively one mission with risk allocated in whatever matter desired as long as the total mission exposure does not exceed the E_C threshold of 30×10^{-6}.

Most ELV operations are launched out over the ocean where the population density is extremely low. ELV safety systems (destructive flight termination systems) are designed to prevent the possibility of the vehicle flying over populated areas for extended periods early in the flight and it is these safety systems that get the most safety scrutiny. In the case of ELVs, other vehicle systems that affect the reliability of the vehicle are less important to safety because a launch vehicle failure over the ocean presents minimal public exposure to risk. Even a relatively high probability of a catastrophic vehicle system failure presents very little safety concern because of the extremely low population densities in the ocean. On the other hand, vehicles that are to be operated over land may expose the public during flight and such measures as performance and reliability of the vehicle and its safety systems all materially affect public safety. This may mean that the level of effort to provide a high level of confidence of system performance and reliability will entail the need for more rigorous analysis and testing. In addition, restrictions, including flight testing over unpopulated or sparsely populated areas, may be needed. The nature of RLVs entail design and performance characteristics that differ from ELVs, such as the reusability factor – flying the same vehicle over and over again, or the concept of new flight safety systems – permitting a vehicle to safely abort its mission during flight under certain circumstances without necessarily requiring its destruction.

---

[1] Expected Casualty (E_C) is used as a measure of public safety and is typically one of the measures used to determine whether a launch should not proceed because of public safety concerns. The measure represents the collective risk measured as expected "average number of casualties" for the specific mission. A tutorial on Expected Casualty can be found in Attachment 2.

[2] The Air Force Range Safety Requirements (EWR 127-1) establishes this risk threshold as a level that if exceeded, higher approval authority is required. To AST's knowledge, no licensed commercial launch has been allowed to proceed which would exceed this threshold for a mission.

Risk Statistics

An E_C risk threshold reflects acceptable collective risk, as opposed to individual annual risk, which describes the probability of serious injury or death to a single person, and is perhaps, the more common measure of risk used in other industries. The launch industry's common measure of risk is collective risk, which may then be measured as individual risk in light of the factors associated with any given launch. Individual risk may be correspondingly less than collective risk, depending on the size of the population exposed. This means that a collective risk of E_C of 30×10^{-6} may be more strict than an individual risk of 1×10^{-6} (1 per million). For example, with a collective risk of 30×10^{-6}, and a population of one hundred thousand exposed to a particular launch, the risk to any one individual is 0.3×10^{-9} (three tenths per billion). For purposes of comparison, the FAA notes that the Air Force describes this collective risk level as no greater than that voluntarily accepted in normal daily activity (Eastern and Western Range 127-1 Range Safety Requirements, Sec. 1.4, 1-12 (Mar. 31, 1995)).

Attachment 2 of this document provides a general description, with simplified examples, of the application of expected casualty to space transportation.

Objective 2: Safety Process Methodology

In addition to the expected casualty objective, an applicant should apply a disciplined, systematic, and logical safety process methodology for the identification and control of hazards associated with its launch and/or reentry systems.

Explanation of Methodology of General System Safety Process:

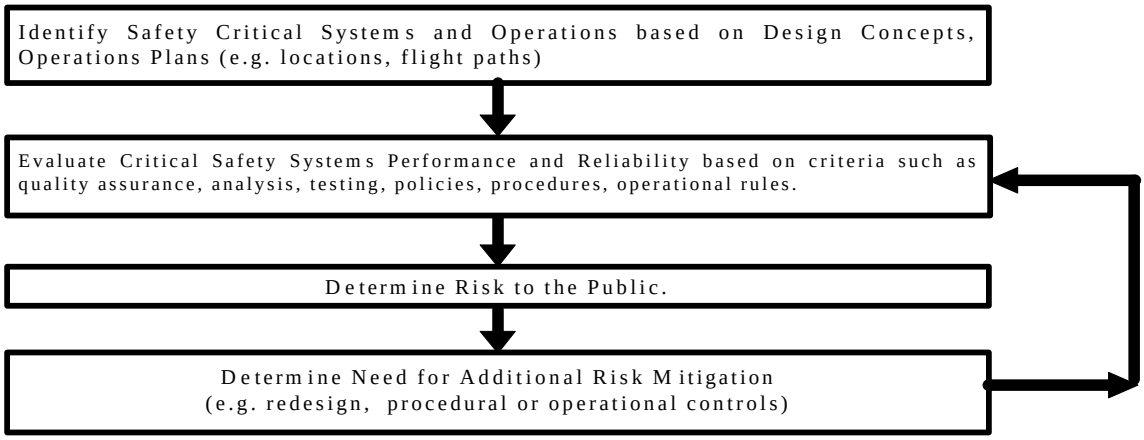

FIGURE 1: SAFETY PROCESS FLOW

The Applicant should use a System Safety Engineering Process or its equivalent, which includes a Risk Analysis, to show that it meets the safety process methodology criteria identified above. The process flow depicted in Figure 1 represents a top level outline of the traditional systems safety engineering process successfully used by DOD and NASA for decades, modified to focus only on risks to public safety. The process depicted is ongoing until all potential risks have been mitigated to an acceptable level. The System Safety Engineering Process used may be similar to that reflected in Military Standard 882C, or the System Safety Analysis Handbook (a System Safety Society Standard), or FAA Advisory Circular "AC No: 25.1309" titled "System Design and Analysis".

The use of a systematic process for the identification and control of safety critical systems and operations also provides the foundation supporting the Expected Casualty analysis. Without a process that helps assure a disciplined approach to the design, manufacture, integration, test, and operation of a system, it will be very difficult to establish any confidence in the probabilities of success and failure provided for the Expected Causality analysis. It is also noted that although the application of a system safety process is extremely important in creating a strong foundation for assuring the safety of a system, it does not in and of itself assure public safety. The combination of the system safety engineering approach with the expected causality analysis and the other applicable objectives in this guidance document is intended to help ensure an adequate level of public safety. See Figure 1B.

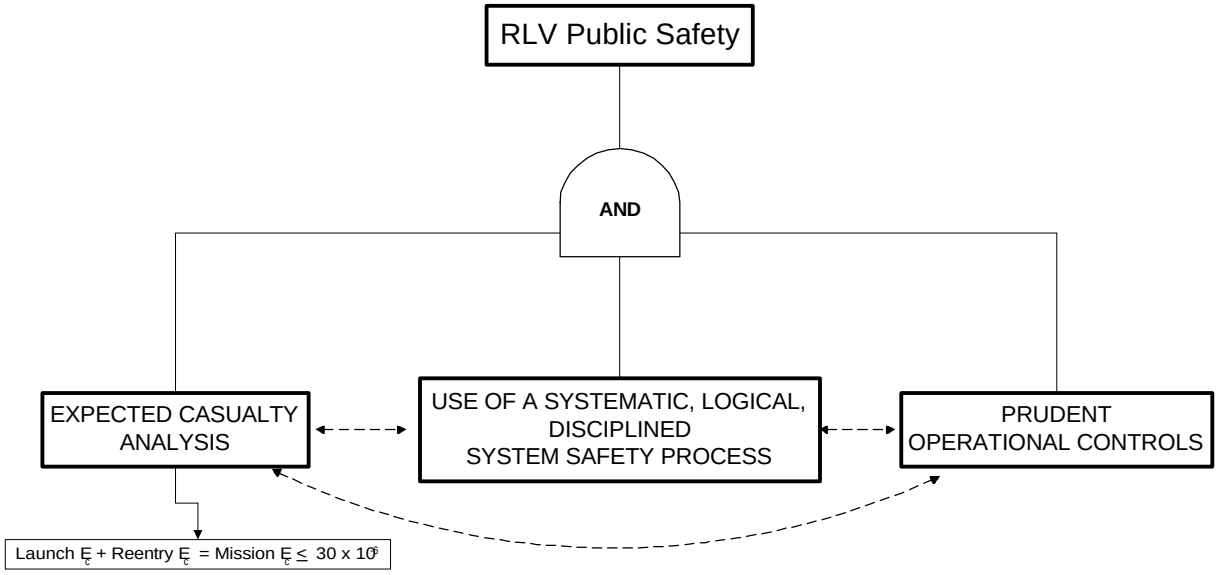

Figure 1B: RLV Public Safety

A more detailed description of the System Safety Engineering Process and a Flow Chart showing the relationship of the process to the system development are included in the attached instructional tutorial (Attachment 1). While Risk Analysis is mentioned in the same attachment, a top-level description with simplified examples of the analysis and measurement of risk (via expected casualty) can be found in Attachment 2. The following is a brief description intended to provide examples of the system safety process and analysis techniques, examples of safety critical systems, and typical analytical and test procedures used to verify safety critical systems and potential operational controls/constraints.

System Safety Engineering Process

The System Safety Engineering Process is the structured application of system safety engineering and management principles, criteria, and techniques to address safety within the constraints of operational effectiveness, time, and cost throughout all phases of the system's life cycle. The intent of the System Safety Engineering Process is to identify, eliminate, or control hazards to acceptable levels of risk throughout a system's life cycle.

This process is performed by the vehicle developer/operator. Because of the complexity and variety of vehicle concepts and operations, only such a process can ensure that all elements affecting public safety are considered and addressed. Without such a process, very detailed requirements would have to be imposed on all systems and operations, to ensure that all potential hazards have been addressed which could have the undesired effect of restricting design alternatives and innovation or could effectively dictate design and operations concepts.

The process (as described in Mil Std 882C, etc.) includes the requirement for a System Safety Program Plan (SSPP). The SSPP (or its equivalent) provides a description of the strategy by which recognized and accepted safety standards and requirements, including organizational responsibilities, resources, methods of accomplishment, milestones, and levels of effort, are to be tailored and integrated with other system engineering functions. The

SSPP lays out a disciplined, systematic methodology that ensures all hazards – all events and system failures (probability and consequence) that contribute to expected casualty – are identified and eliminated, or that their probability of occurrence is reduced to acceptable levels of risk (per objective 1,6,8, and 10).

The SSPP should indicate the methods employed for identifying hazards such as Preliminary Hazards Analysis (PHA), Subsystem Hazard Analysis (SSHA), Failure Mode and Effects Analysis (FMEA), Fault Tree Analysis, etc. Risk Mitigation Measures are likewise identified in the plan. These include avoidance, design/redesign, process/procedures and operational rules and constraints.

Identification of Safety Critical Systems

For the purposes of a System Safety Engineering Process safety critical systems are defined as any system or subsystem whose performance or reliability can affect public health, safety and safety of property. Such systems, whether they directly or indirectly affect the flight of the vehicle, may or may not be critical depending on other factors such as flight path and vehicle ability to reach populated areas. For this reason it is important to analyze each system for each phase of the vehicle mission from ground operations and launch through reentry and landing operations. Examples of potentially safety critical systems that may be identified through the system safety analysis process using PHA or other hazard analysis techniques may include, but are not limited to:

- Structure/integrity of main structure
- Thermal Protection System (e.g., ablative coating)
- Temperature Control System (if needed to control environment for other critical systems)
- Main Propulsion System
- Propellant Tanks
- Power Systems
- Propellant Dumping System
- Landing Systems
- Reentry Propulsion System
- Guidance, Navigation and Control System(s), Critical Avionics (Hardware and Software) - This includes Attitude, Thrust and Aerodynamic Control Systems
- Health Monitoring System (hardware and software)
- Flight Safety System (FSS)
- Flight Dynamics (ascent and reentry) for stability (including separation dynamics) and maneuverability
- Ground Based Flight Safety Systems (if any) including telemetry, tracking and command and control systems
- Depending on the concept, additional “systems” might include pilot and life support systems and landing systems if they materially affect public health and safety
- Others identified through hazard analysis

Validation of Safety Critical Systems

An Applicant should be able to demonstrate that the proposed vehicle design and operations will satisfy the safety objectives of this guidance material and that the system will survive and perform safely in all operating environments including launch, orbit, reentry and recovery. Documentation should show adequate design, proper assembly, and vehicle control during all flight phases. Documentation is expected to consist of design information and drawings, analyses, test reports, previous program experience, and quality assurance plans and records.

The FAA uses a pre-application consultation process to help a potential applicant to understand what must be documented and to help identify potential issues with an applicant's proposed activities that could preclude its obtaining a license. This process is especially important for RLV systems because most are using unique technology and operating concepts. The pre-application process should be initiated by the applicant early in their system development (if possible during the operations concept definition phase) and maintained until their formal license application is completed. This pre-application process should be used to provide the FAA with an understanding of the safety processes to be used, the safety critical systems identified, analysis and test plan development, analysis and test results, operations planning, flight rules development, etc. As a function of the pre-application process the FAA may attend design reviews and system tests, in order to ensure that development, testing and test results are consistent with the analyses, and other demonstrations made to the FAA. See Attachment 1 for additional information.

Analyses may be acceptable as the primary validation methodology in those instances where the flight regime cannot be simulated by tests, provided there is appropriate technical rationale and justification.

Qualification tests, as referenced in the Safety Demonstration Process and the System Safety Program Plan, are normally conducted to environments higher than expected. For example, ELVs' Flight Safety Systems (FSS) are qualified to environments a factor of two or higher than expected. (See Figure 2)

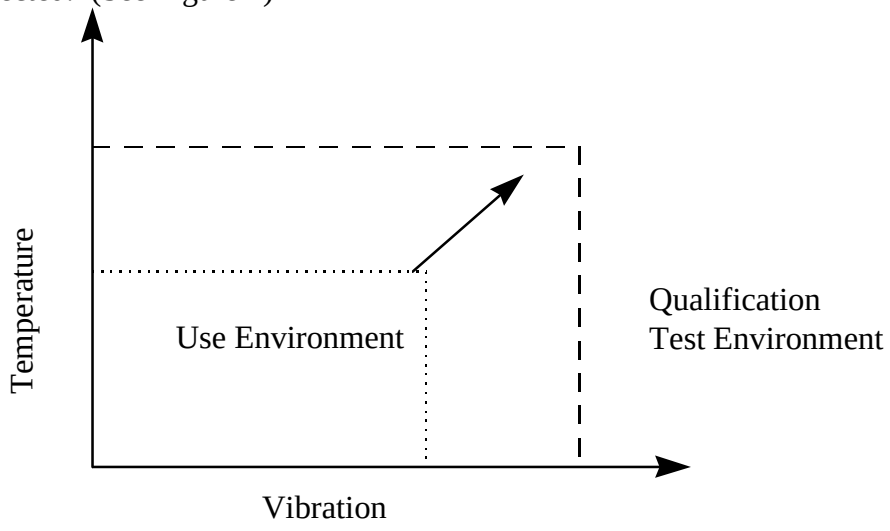

Figure 2. Relationship of Use Environment to Qualification Test Environment

These tests are conducted to demonstrate performance and adequate design margins and may be in the form of multi-environmental ground tests, tests to failure, and special flight tests. Such tests are normally preceded with detailed test plans and followed by test reports.[3] In addition, Quality assurance (QA) records help establish verification of both design adequacy and vehicle assembly and checkout (workmanship).

The following matrix identifies examples of approaches that may be employed to validate acceptance for critical systems. Examples of types of analyses, ground tests, and flight tests are provided following this matrix. (Note: Quality Assurance programs and associated records would be essential where analysis or testing, covering all critical systems, are involved.)

Candidate Critical Systems	Analyses	Ground Test	Flight Test
Structure/Integrity of Main Structure	X	X	P
Thermal Protection	X	P	P
Environmental Control (temp, humidity)	X	X	X
Propulsion: Main, Auxiliary and Reentry (de-orbit)	X	P	P
Propellant Tank Pressurization	X	X	P
GN&C, Critical Avionics *; includes de-orbit targeting (e.g., star-tracker, GPS)	X	X	X
Health Monitoring *	X	X	X
Flight Safety System (FSS)*	X	X	X
Recovery and Landing	X	P	P
Ordnance (other than Safety)	X	X	X
Electrical and Power	X	X	X
Telemetry and Tracking and Command*	X	X	X
Flight Control (ascent, separation, reentry) *	X	X	X
FSS Ground Support Equipment (if any) *	X	X	N/A

P - partial; cannot satisfy all aspects
X - if in sufficient detail when combined with test results or selected analyses

- - includes both hardware and software

[3] Test plans are important elements of the ground and flight test programs. Such plans define, in advance, the nature of the test (what is being tested and what the test is intended to demonstrate with respect to system functioning, system performance and system reliability). The test plan should be consistent with the claims and purpose of the test and wherever appropriate, depending on the purpose of the test, clearly defined criteria for pass and fail should be identified. A well defined test plan and accompanying test report may replace observation by the FAA.

Analyses

There are various types of analyses that may be appropriate to help validate the viability of a critical system or component. The following provides examples of some types of critical systems analysis methodologies and tools. Again these are *only examples* and should not be construed as the only analyses or software tools which may be necessary to validate a specific system for a specific operational environment, nor should it be interpreted that all of these example analysis and software tools will be necessary to validate a specific system.

Mechanical Structures and Components (Vehicle Structure, Pressurization, Propulsion System including engine frame thrust points, Ground Support Equipment)

- Types of Analyses: Structural Loads, Thermal, Fracture Mechanics, Fatigue, Form Fit & Function
- Software Tools for Analyses: Nastran, Algor, Computational Fluid Dynamics codes, CAD/CAM

Thermal Protection System

- Types of Analyses for TPS and Bonding Material: Transient and Steady State Temperature Analyses, Heat Load, and Heating and Ablative Analyses.
- Software Tools for Analyses: SINDA by Network Analysis Inc.

Electrical/Electronic Systems & Components (Electrical, Guidance, Tracking, Telemetry, Navigation, Communication, FSS, Ordnance, Flight Control and Recovery)

- Types of Analyses: Reliability, FMEA, Single Failure Point, Sneak Circuit, Fault Tree, Functional Analysis, Plume effects
- Software Tools for Analyses: MathCad, Relex, FaultrEase

Propulsion Systems (Propulsion, FSS, Ordnance, Flight Control)

- Types of Analyses: Analytical Simulation of nominal launch and abort sequences for Main Engines, Orbital Maneuvering System (including restart for reentry-burn) and Attitude Control System; capacity analysis for consumables; Plume Flow Field Modeling
- Software Tools for Analyses: Nastran, Algor, SPF-III, SINDA

Aerodynamics (Structure, Thermal, Recovery)

- Types of Analyses: Lift, Drag, Stability, Heating, Performance, Dispersion, Plume effects
- Software Tools for Analyses: Post 3/6 DOF, Computational Fluid Dynamics Codes, Monte Carlo Simulation Codes

Software (Guidance, Tracking & Telemetry & Command, FSS, Flight Control and Recovery)

- Types of Analyses: Fault Tree, Fault Tolerance, Software Safety (including abort logic), Voting Protocol Dead Code, Loops, and Unnecessary Code
- Validation Methodologies, such as ISO 9000-3 [4]

[4] ISO 9000-3 is used in the design, development, and maintenance of software. Its purpose is to help produce software products that meet the customers' needs and expectations. It does so by explaining how to control the quality of both products and the processes that produce these products. For software product

Ground Tests

Ground tests include all testing and inspections performed prior to flight, including qualification, acceptance and system testing. It is anticipated that an applicant will perform various types of ground tests to validate the capability of critical systems and components. The following provides examples of some types of critical systems validation ground tests. Again these are *only examples* and should not be construed as the only types of ground tests which may be necessary to validate a specific system for a specific operational environment, nor should it be interpreted that all of these example ground tests will be necessary to validate a specific system.

Mechanical Systems and Components (Vehicle Structure, Pressurization, Propulsion System including engine frame thrust points, Ground Support Equipment)

- Types of Tests: Load, Vibration (dynamic and modal), Shock, Thermal, Acoustic, Hydro-static, Pressure, Leak, Fatigue, X-ray, Center of Gravity, Mass Properties, Moment of Inertia, Static Firing, Bruceton Ordnance, Balance, Test to Failure (simulating non-nominal flight conditions), Non-Destructive Inspections

Electrical/Electronic Systems (Electrical, Guidance, Tracking, Telemetry and Command, Flight Safety System (FSS), Ordnance, Flight Control and Recovery)

- Types of Tests: Functional, Power/Frequency Deviation, Thermal Vacuum, Vibration, Shock, Acceleration, X-ray, recovery under component failures, abort simulations, TDRSS integration testing (up to and including pre-launch testing with flight vehicle)

Propulsion Systems (Propulsion, FSS, Ordnance, Flight Control)

- Types of Tests: Simulation of nominal launch and abort sequences for engines (including restart, if applicable), Orbital Maneuvering System (including restart for reentry-burn) and Attitude Control System; Environmental testing (Thermal, Vibration, Shock, etc.)

Thermal Protection System

- Types of Tests (for TPS and bonding material): Thermal, Vibration, Humidity, Vacuum, Shock

Aerodynamics (Structure, Thermal, Recovery)

- Types of Tests: Wind Tunnel, Arc Jet, Drop Tests (Landing Systems)

Software (Electrical, Guidance, Tracking, Telemetry, Command, FSS, Ordnance, Flight Control and Recovery)

- Types of Tests: Functional, Fault Tolerance, Cycle Time, Simulation, Fault Response, Independent Verification and Validation, Timing, Voting Protocol, Abort sequences (flight and in-orbit) under non-nominal conditions with multiple system failures, Integrated Systems Tests

---

quality, the standard highlights four measures: specification, code reviews, software testing and measurements.

Flight Tests

Flight testing is very valuable to the space vehicle development process. As the RLVs complete engineering and safety analyses and ground testing, considerable planning is needed to define the flight test program that will establish the performance capabilities of the vehicle for routine and repetitive commercial operations. When flight testing is required, a flight test plan will be needed to demonstrate that the RLV's proposed method of operations is acceptable and will not be a hazard to the public's health, safety and safety of property.

The purpose of flight testing is to verify the system performance, validate the design, identify system deficiencies, and demonstrate safe operations. Experience repeatedly shows that while necessary and important, analyses and ground tests, cannot and do not uncover all potential safety issues associated with new launch systems. Even in circumstances where all known/identified safety critical functions can be exercised and validated on the ground, there is still the remaining concern with unrecognized or unknown interactions ("the unknown unknowns").

Flight tests should be conducted in a manner such that the vehicle and its instantaneous impact point never overfly populated areas. This permits the safe demonstration of the vehicle without posing a significant public safety hazard. The structure of the test program will identify the flight test framework and test objectives, establish the duration and extent of testing; identify the vehicle's critical systems, identify the data to be collected, and detail planned responses to nominal and unsatisfactory test results.

Test flight information includes verification of stability, controllability, and the proper functioning of the vehicle components throughout the planned sequence of events for the flight. All critical flight parameters should be recorded during flight. A post-flight comparative analysis of predicted versus actual test flight data is a crucial tool in validating safety critical performance. Below are examples of items from each test flight that may be needed to verify a reusable launch vehicle. Listed with each item are examples of what test-flight data should be monitored or recorded during the flight and assessed post-flight:

- Vehicle/stage launch phase: Stability and controllability during powered phase of flight.
  - Vehicle stage individual rocket motor ignition timing, updates on propellant flow rates, chamber temperature, chamber pressure, and burn duration, mixture ratio, thrust, specific impulse (ISP)
  - Vehicle stage trajectory data (vehicle position, velocity, altitudes and attitude rates, roll, pitch, yaw attitudes)
  - Vehicle stage Attitude, Guidance and Control system activities
  - Functional performance of the Vehicle Health Monitoring System
  - Functional performance of the Flight Safety System/Safe Abort System
  - Electrical power, and other critical consumables, usage and reserves (i.e. gases, fluids, etc…)
  - Actual thermal and vibroacoustic environment
  - Actual structural loads environment

- Staging/separation phase of boost and upper stages: Stable shutdown of engines, and nominal separation of the booster & upper stages.
  - Separation activity (timestamp, i.e., separation shock loads, and dynamics between stamps)
  - Functional performance of the Vehicle Health Monitoring System
  - Electrical power, and other critical consumables, usage and reserves (i.e. gases, fluids, etc…)
  - Functional performance of the Flight Safety System/Safe Abort System
- Booster stage turn-around (re-orientation) or "loft" maneuver phase (if applicable).
  - Rocket motor re-start (if applicable): timing, updates on propellant flow rates, chamber temperature, chamber pressure, burn duration, mixture ratio, thrust, ISP
  - Attitude, Guidance and Control system activities
  - Actual structural loads environment
  - Actual thermal and vibroacoustic environment
  - Functional performance of the Flight Safety System/Safe Abort System
- Booster stage flyback phase (if applicable): Flyback engine cut-off, fuel dump or vent (if required), nominal descent to the planned impact area, proper functioning and reliability of the RLV landing systems.
  - Booster stage post-separation (flyback) trajectory data
  - Electrical power usage and reserves
  - Booster stage landing system deployment activity (timestamp)
  - Actual thermal and vibroacoustic environment
  - Actual structural loads environment
  - Functional performance of the Vehicle Health Monitoring System
  - Functional performance of the Flight Safety System/Safe Abort System
  - Attitude, Guidance and Control system activities
- Vehicle stage ascent phase (if multistage): nominal ignition of the stage's engine, stability and controllability of the stage during engine operation, orbital insertion – simulated (for suborbital) or actual – of the vehicle.
  - Vehicle individual rocket motor ignition timing, updates on propellant flow rates, chamber temperature, chamber pressure, and burn duration
  - Vehicle circularization and phasing burn activities (ignition timing, updates on propellant flow rates, chamber temperature, chamber pressure, and burn duration)
  - Vehicle trajectory data (vehicle position, altitude, velocity, roll, pitch, yaw attitudes at a minimum)
  - Attitude, guidance and control system activities
  - Functional performance of the Vehicle Health Monitoring System

  - Functional performance of the Flight Safety System/Safe Abort System
  - Electrical power, and other critical consumables, usage and reserves (i.e. gases, fluids, etc…)
  - Actual structural loads environment
  - Actual thermal and vibroacoustic environment

- Vehicle descent (including vehicle's de-orbit burn targeting and execution phases): Function of the programmed flight of the vehicle/upper stage to maintain the capability to land (if reusable) at the planned landing site, or to reenter for disposal (if expendable), assurance of fuel dump or depletion, and proper descent and navigation to the planned or alternate landing site.
  - Vehicle pre-deorbit burn trajectory data
  - Vehicle deorbit burn data (ignition timing, updates on propellant flow rate, chamber temperature, chamber pressure, and burn duration)
  - Vehicle descent trajectory data (position, velocity, and attitude)
  - Attitude, Guidance and Control system activities
  - Actual thermal and vibroacoustic environment
  - Actual structural loads environment
  - Functional performance of the Vehicle Health Monitoring System
  - Functional performance of the Flight Safety System/Safe Abort System
  - Electrical power and other critical consumables usage and reserves (i.e. gases, fluids, etc…)
  - Vehicle landing system deployment activity (timestamp)

Performance and Reliability Data

Performance and reliability data may be supported by flight history on other vehicles with similar or comparable safety critical systems, sub-systems, and components, and by conducting both analyses and tests, at the respective levels. Having a flight history could mean extensive documentation may not be required if it can be shown through test results, analyses, or empirical data, that the flight regimes experienced are similar to the proposed flight regime. The degree of applicability of data depends on the degree of similarity to environmental conditions and how environmental conditions compare to the history and anticipated reactions of this system. Even when the same system, sub-system, or component is known to have an extensive (and favorable) flight history in the same or more severe environments, interfaces and integration with other systems would still be examined and tested. Another method of acquiring data is through estimating system, sub-system, and component 3-sigma performance and reliability numbers from testing evaluations and (where applicable) flight data.

The use of similarity is not new to launch operations. EWR 127-1, para. 4.14.1.2, states: as required, qualification by similarity analysis shall be performed; if qualification by similarity is not approved, then qualification testing shall be performed. For example, if component A is to be considered as a candidate for qualification by similarity to a component B that has

already been qualified for use, component A shall have to be a minor variation of component B. Dissimilarities shall require understanding and evaluation in terms of weight, mechanical configuration, thermal effects, and dynamic response. Also, the environments encountered by component B during its qualification or flight history shall have to be equal to or more severe than the qualification environments intended for component A.

Operational Controls

There is an interrelationship between the system design capabilities and the systems operational limitations. Figure 3 depicts the relationship between the vehicle systems and the scope of operations within which the vehicle is operated. What constitutes a safety critical system may depend on the scope and nature of the vehicle design and its proposed operations. Intended operational requirements affect the proposed vehicle design requirements and vehicle capabilities/limitations and also establish the operational system constraints necessary to protect public health and safety. For example, landing sites may have to be within some minimum cross-range distance from the orbital ground trace because of cross-range limitations of the vehicle. A vehicle operator may choose, or be required, to mitigate certain vehicle limitations through the use of operational controls rather than relieving vehicle limitations through design changes.

Test parameters and analytic assumptions will further define the limits of flight operations. The scope of the analyses and environmental tests, for example, will constitute the dimensions of the applicant's demonstration process and therefore define the limits of approved operations if a license is issued. Such testing limits, identified system and subsystem limits, and analyses also are expected to be reflected in mission monitoring and mission rules addressing such aspects as commit to launch, flight abort, and commit to reentry.

Vehicle capabilities/limitations and operational factors such as launch location and flight path each affect public risks. The completion of system operation demonstrations, such as flight simulations and controlled flight tests, provide additional confidence in the vehicle systems and performance capabilities. As confidence in the systems overall operational safety performance increases, key operational constraints such as restrictions on overflight of populated areas may be relaxed.

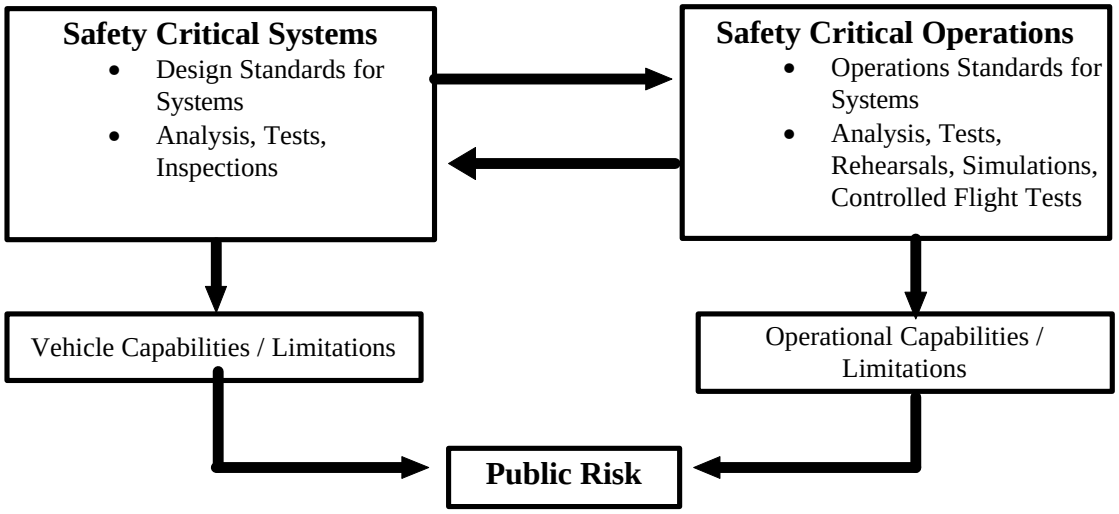

FIGURE 3: INTERRELATIONSHIP BETWEEN SAFETY CRITICAL SYSTEMS AND OPERATIONS

The following are examples of the types of operations-related considerations that may need to be addressed by the applicant when establishing their operations scenarios.

- Launch commit criteria/rules
- Human override capability to initiate safe abort during launch and reentry
- System monitoring, inspection and checkout procedures
- For reflight: inspection and maintenance
- Selected primary and alternate landing sites for each stage
- Surveillance/control of landing areas
- Standard limits on weather
- Coordination with appropriate air space authorities
- Limits on flight regime (ties in with analysis, testing and demonstrating confidence in system performance and reliability)
- Limits on over-fight of populated areas
- Others identified through hazard analysis

Objective 3: Human Intervention Capability During the Ascent To Orbit Phase for Orbital Missions, and throughout the entire mission (ascent and descent), for Sub-orbital Launches of Reusable Launch Vehicles

Risks to the public from non-nominal launches should be mitigated through control based on human decision making or intervention in addition to any on-board automatic abort system. The specific flight safety systems design involving ground, airborne or on-board capability should assure the redundant ability to initiate a safe abort of a malfunctioning RLV.

Discussion:

ELVs and conventional aircraft incorporate human decision making in conjunction with on-board automatic systems to ensure public safety if a non-nominal event regarding the vehicle occurs. Most ELV safety systems have over 40 years of operational history and proven reliability and are relatively simple in design. The majority of ELV safety systems are destructive (explosive) and are designed to be used over unpopulated areas such as broad ocean areas where the vehicle debris impacts do not affect public health and safety. However, most RLV safety systems will not have the benefit of low operating risk and high confidence levels associated with the experience and flight history of ELV Flight Termination Systems. Without considerable testing, including flight tests, it may be difficult to establish autonomous RLV Flight Safety System reliability with adequate confidence to permit overflight of populated areas. These sophisticated RLV safety systems may be expected to monitor and address a myriad of possible systems failures. The RLV safety system will be required to respond appropriately to these system failures and provide a level of public safety that is at least equivalent to the level of public safety provided by ELV safety systems. Providing human control, at least through an override capability to the RLV safety system, should lower that system's operational risk. Therefore, a human operator should have the ability to monitor the status of the vehicle during ascent and at other critical times (as per. Objective 5) in order to independently initiate abort actions should it be necessary.

Objective 4: Positive Human Initiation of Reentry Activities

Risks to the public from non-nominal reentries should be mitigated through control based on human enable of the reentry activity. This objective is intended to provide fail-safe assurance that reentry activities cannot be initiated prior to human verification that all pre-reentry readiness activities, including verifying the configuration and status of reentry safety critical systems.

Discussion:

Depending on system design and operations concepts, it is anticipated that there will be a number of activities that will need to be completed, prior to the initiation of reentry operations, to assure that a reentering vehicle will not pose significant risks to the public. These activities may include clearing airspace in the reentry corridor, securing reentry-landing sites, verifying the configuration and status of reentry safety critical vehicle systems, verifying reentry corridor weather is within vehicle operational constraints, etc.

Some of these activities are independent of the vehicle systems and as a result autonomous control systems would not consider them. Therefore, a human operator should have the ability to monitor the status of the vehicle reentry safety critical systems prior to initiating reentry operations.

Objective 5: Flight Data Monitoring and Recording

The RLV and ground support systems should provide for sufficient flight data monitoring such that the status of key systems is provided during the entire launch phase of the mission and at the other safety critical mission decision points. This may be done through telemetry, in real time, to a control center which has command capability and decision making responsibility. Other data that is not essential to be monitored in real time but for which monitoring or verification is necessary for system validation, system reuse, performance characterization, etc., could be recorded onboard for non-real time download or retrieval post-mission.

Discussion:

In order to provide the human intervention capability during the launch phase as described in objective 3, and the fail safe enable of reentry operations as described in objective 4, a level of flight data monitoring would be necessary. The specifics of which data will need to be monitored and when it will need to be available will be dependent on vehicle systems and operating concepts. In addition, the whole premise of RLV vehicles is reusability of the vehicle and the premise of flight tests is to learn more about the performance of the on-board systems and the actual operating environment. Such data is critical to providing the confidence needed to expand the test flight envelope, and could be gathered and provided via telemetry for review and analysis while the vehicle is still in flight or retrieved post flight. Regarding real time and non-real time (down-loading stored data) telemetry, the categories fall into information that is crucial for determining vehicle safety and performance status (real time), and information which is compiled by the vehicle for which there is no requirement for immediate (real time) access (thus non-real time would be acceptable).

Objective 6: Non-nominal Reentry Risk Mitigation

RLVs designed to re-enter from orbit and survive substantially intact should not produce a total public casualty expectancy (E_C) greater than $30x10^{-6}$ as a result of nominal or non-nominal launch and reentry operations.

Discussion:

All things placed into earth orbit will eventually reenter the earth's atmosphere[5]. This is because their orbits decay due to a number of factors including atmospheric drag and

[5] Anything placed in earth orbit will eventually decay. All orbiting objects have some rate of decay, not just LEO but up to and including Geo-Synchronous Orbits (GEO).

magnetic forces. The length of time it takes depends on the size of the object and the altitude and eccentricity of the orbit. Generally, the lower the orbit, the less time it takes for the object to decay out of orbit. Normally, spacecraft and launch vehicle stages inserted into orbit are not designed to survive reentry and all, or nearly all, of their components are vaporized before impacting the earth because of the high temperatures encountered as they pass through the atmosphere. RLV reentry stages that are protected from these high temperatures for recovery, may survive a non-nominal or random reentry intact unless preventive measures are taken.

After reaching orbit, if a decision is made that commanded reentry towards the landing site will not be attempted, the vehicle will eventually reenter randomly as the vehicles orbit naturally decays, unless a commanded reentry is performed for the purpose of disposing of the vehicle in a remote ocean area. The intent of this objective is to ensure reentering RLV bodies pose no more risk[6] than other stages and payloads that reenter and, if necessary, can be completely destroyed by normal reentry heating and loads.

This objective allows for the use of planned sites which may include alternate sites, such as a broad ocean area, when circumstances are such that while reentry can be initiated, there is not sufficient controllability to land in a relatively small area because of system failures or other detected degradation of system performance.

Incorporating the ability to destroy the heat shield effectiveness in a random reentry condition may also satisfy this objective. That is, provide for the ability to significantly mitigate the risk under the circumstances of a random reentry situation by disabling or otherwise compromising the effectiveness of the thermal protection system (TPS). Aside from destructing the vehicle during reentry, some limited type of action may be sufficient to breach a portion of the TPS of the vehicle. Its integrity compromised, the vehicle would burn up upon reentry. Such actions may include consideration of opening payload compartment doors, reorienting the vehicle attitude, breaching, removing or otherwise rendering key areas of the TPS ineffective.

Objective 7: Overflight of Populated Areas

RLV flight over land corridors should be selected such that any land overflight avoids densely populated areas. Determinations of population densities for such areas are based on a density that is dependent on the casualty area from each RLV configuration, and may differ for each case.

Discussion:

RLVs by their very nature are experimental, utilize unproven systems and operating concepts, and have the potential for catastrophic failures that could negate their ability to abort safely. The

[6] During the approval process for the COMET/METEOR reentry vehicle, one of the safety issues addressed by the DOT was the risk to the public if the decision was made, because of system problems, to not attempt a reentry. In this case the reentry vehicle's debris (even if the vehicle survived completely after its orbit decayed), was less than that believed to survive from many ELV stages. This may not be the case for RLVs because of their size.

intent of this objective is to limit the potential of a catastrophic consequence involving a potentially large number of public casualties, even though the computed risk of such an occurrence may be much lower than the risk objective[7]. This standard is similar to the restrictions placed on experimental aircraft and aircraft flight testing.

Consideration has been given to establishing a fixed population density value; however, assigning such a value may be inappropriate because there are many configurations and sizes of proposed RLVs. Population density limits would be dependent on the casualty area from each RLV configuration, and therefore would differ for each case. Each RLV configuration would thus be evaluated for its maximum probable impact in a non-nominal situation. That maximum probable impact data would then be used along with the Ec requirement to solve for the maximum allowable population density for overflight. Each vehicle would therefore have a different overflight constraint.

Objective 8: Reentry/Landing Site Risks

The public located in proximate vicinity to the planned reentry site should not be exposed to an unreasonable risk as a result of RLV operations. For nominal missions, the predicted 3-sigma dispersion of a RLV reentry vehicle during descent (landing) operations will be wholly contained within the planned landing site.

Additionally, it is a goal that the risks to the public from such a nominal reentry shall not exceed an E_C of $1x10^{-6}$ for areas surrounding the site.[8]

Discussion:

Reentry systems must land at designated locations and the size of the landing sites must be sufficient to accommodate the characteristics of the vehicle. Depending on the vehicle and its capability to adjust its landing point and the accuracy of the landing systems, the size of the landing footprint can vary. It is the intent of this objective to ensure that, for nominal operations, the 3-sigma landing footprint of the vehicle be contained within the controlled landing site.

This objective is based on nominal performance of the vehicle and does not include the impacts of system failures. It is directed at the nominal flight capabilities of the vehicle and the demonstration that the controlled landing site is of sufficient size to accommodate the vehicle. (The possible impacts of system failures during reentry operations will be addressed in the reentry Expected Casualty analysis.) This objective does not impose severe restraints on reentry site selection unless the reentry dispersion is large.

[7] If the collective risk for the mission has an expected casualty of 30×10^{-6}, the risk of 30 casualties occurring in a single event, for example, will be far less, approximately 1×10^{-7}.

[8] For example: In COMET/METEOR, the surrounding area was defined as that area within 100 miles of the landing site.

Objective 9: Preplanned, Pre-approved Staging Impact Points, Contingency Landing Sites and Contingency Abort Sites

For launch and reentry operations, RLV operators would provide staging impact points and, at selected points along its overflight corridor, safe, pre-planned, pre-approved[9] contingency abort landing sites. These sites must be large enough to ensure that all RLV landing hazards are contained within the designated site. There should be a sufficient number and distribution of such sites to assure abort to these sites (or to orbit) can be achieved from any phase of the flight. These sites should avoid air traffic routes or mitigation measures could be taken to ensure there are no aircraft over the site at the time of reentry.

Discussion:

Conventional aircraft are operated in a manner that requires the aircraft to abort the flight and land at the nearest suitable airport whenever critical flight safety systems malfunction. Expendable Launch Vehicles (ELV) currently operate primarily over broad ocean areas only sparsely populated by shipping. The current practice is to contain a malfunctioning ELV within these broad ocean areas through the use of both on-board automatic and ground commanded systems. Similarly, continuing flight of a malfunctioning RLV may not be permitted. An abort executed to a safe landing site may be necessary just as it is for conventional aircraft. One of the major risk mitigation attributes of RLVs is that should a malfunction occur and the event is not a catastrophic failure, the vehicle will abort the flight allowing the recovery of the vehicle and payload intact while not endangering the public.[10] Therefore, it may be prudent to provide the (contingency) capability to safely abort to a landing site and to ensure that the landing site can safely accommodate the vehicle.

Just as occurs for ELV launches, RLVs will need to establish exclusion areas for aircraft. Such areas are monitored and should an aircraft be within the area, the launch and/or reentry is delayed until the area is clear. Another risk mitigation technique is the issuance of notices for stage impact areas. In the case of RLVs such actions are appropriate for launches as well as the planned, primary and alternate, landing sites.

Objective 10: Flight Test Demonstration Program

Inland populations should not be exposed to unreasonable risk of harm from unproven RLV systems.

RLVs that are intended to operate from inland sites involving substantial overflight of populated areas to achieve their mission, should perform a flight test demonstration

[9] "Approval" refers to any approval by the FAA with respect to the proposed sites meeting the requirements otherwise stated in this (or similar document) as well as any other state and local entities that may have regulations covering the use of such sites.

[10] At some stage in the flight the vehicle may also safely abort to orbit before attempting a reentry to a landing site. The number of sites will depend on the vehicle's capabilities but may include the launch site as well as one or more down range sites.

program.[11] Test flights can demonstrate that the RLV can perform the critical abort and recovery maneuvers necessary to fly safely over populated areas. Flight test demonstrations would be conducted over unpopulated areas or over areas so sparsely populated that the acceptable risk levels of $E_C < 30x10^{-6}$ can be achieved assuming a probability of failure = 1 while over the populated area.

Discussion:

Flight testing is typically performed in order to learn more about system performance and implies a higher level of uncertainty and potential for a failure. There are ways of conducting flight tests to ensure that the public is not exposed above a minimum safety threshold. New ELVs conduct their first flights at ranges where the ability to contain the adverse effects of a malfunctioning vehicle is ensured such that the effect will not reach public areas. RLVs which want to eventually operate for some period over populated areas from lift-off to orbital insertion or from de-orbit through landing, may be required to perform flight demonstration tests to ensure public safety. The extent of such RLV test flights (e.g., suborbital or orbital) will depend on the ability to contain and limit exposure to the specified limit.[12] Most RLVs propose to operate over populated areas, and are relying heavily on Flight Safety Systems to provide a (contingency) safe abort capability to achieve required safety levels. The performance and reliability of such flight safety systems, as well as other systems, become an important element to safety demonstrations. It is very unlikely that sufficient confidence in such system's performance and reliability can be achieved solely through analysis and ground tests. Therefore, it may be necessary that part of the demonstration process include controlled flight tests. Because flight testing is part of the demonstration process to verify the performance and capabilities of safety critical systems, is it important, given the limited confidence prior to such tests of new, unproven vehicles, that flight tests be conducted at a reduced collective risk level. (i.e. $E_C < 30 \times 10^{-6}$ using a probability of failure = 1)
For example, for a vehicle with a casualty area of 5,000 square feet, that would effectively limit the areas exposed to a population density of less than 0.16 people per square mile.

Unlike aircraft, where there have been hundreds of thousands of aircraft systems (e.g., jet turbine engines) produced and flown, this is not the case for the proposed reusable launch vehicles. New aircraft typically go through a flight test program during which the functioning and performance of the aircraft and systems are checked out in a flight environment *before* they are permitted to fly over densely populated areas.

While many of the major systems of an RLV may be unique, it is often the case that such systems are created using subsystems and components for which there is some

[11] More stringent safety operational standards may be appropriate to allow the first test flight to be orbital. For example conditions, such as oceanic reentry, may apply. Initial test flights not involving overflights of populated areas (e.g., coastal-over water or suborbital - within the confines of an unpopulated area) may be permitted, if it can be demonstrated that the vehicle will stay within the confines of the unpopulated area at all times. An example may be the utilization of a flight termination system and predefined destruct lines such that it prevents the vehicle/debris instantaneous impact point (IIP) from passing over populated areas..

[12] There may be circumstances where the intent of the proposed objective for test demonstration flights is clearly achieved without such tests. The nature of such conditions is not clearly defined and would be based on the specific circumstances including the population exposed, the degree of analyses and other testing conducted and the confidence that could be placed in such demonstrations. These circumstances would be addressed on a case-by-case basis.

performance and reliability experience. The usefulness of such information is dependent on whether the experience is associated with similar environments and operational profiles. In addition, there may be issues associated with the interfaces and interactions between subsystems/components.

While many tests can be conducted on a system level on the ground (e.g., much like turbine engine test stands for testing aircraft engines after a major overhaul), it may be necessary to conduct RLV flight tests in order to test all the systems and their interactions in a flight environment.

The FAA may consider licensing a sequence or series of test flights as long as the flight test operations are maintained within an envelope of approved parameters.

Objective 11: Preflight Inspection and Checkout

Prior to each flight, RLVs should undergo system monitoring, inspection and checkout to ensure that all critical systems are functioning within intended parameters and are not otherwise impaired or degraded.

Discussion:

Due to the inherent risks of operating RLV's, it is necessary to verify that all launch and reentry safety critical systems are functioning properly prior to launch. This type of pre-operations verification and checkout has been a standard practice in the aircraft and space launch industries since their inception. Even for test flights, it is important for safety to ensure the systems are functioning properly before each flight. The purpose of test flights is to demonstrate and measure the performance and functioning of key systems. Such information may not be of great value if the condition of the system being tested is not clear. Such information will provide valuable documentation on how the critical systems hold up to the flight environment and the cycling of loads on the vehicle due to reusability. Unanticipated problems may be uncovered during this process which, if not corrected, might lead to serious public health and safety consequences. The vehicle developer and operator should define a preflight validation and checkout process/procedure that meets the intent of this objective.

Attachments
Other Support Information